



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

fw

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,771	02/28/2002	James D. Crumly	10015964-1	8952
7590	02/10/2006		EXAMINER	
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			TESLOVICH, TAMARA	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/086,771	CRUMLY ET AL.
	Examiner	Art Unit
	Tamara Teslovich	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 01 November 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-30 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

This action is in response to the Applicant's Remarks and Amendments filed November 1, 2005.

Claim 12 has been amended.

Claims 1-30 are herein considered.

Response to Arguments

Applicant's arguments filed November 1, 2005 have been fully considered but they are not persuasive.

The Applicant argues on page 8 of his amendment that Manico and Schneier fail to teach or suggest (1) encrypting the digital image with the identified public key or (2) digitizing a physical tag to create a digital tag readable to identify a public key. The applicant specifically claims that the Examiner has asserted that Manico discloses a method of encrypting an image. The Examiner would like to draw the Applicant's attention to page 3 of the previous office action wherein the Examiner specifically states on the last line of the page that 'Manico fails to disclose encrypting the digital image with the identified public key' and then goes on to explain on page 4 how Schneier is relied upon to teach such a method, followed closely by the reasons for combining the two.

As per the Applicant's arguments that Manico's 'security code' fails to identify a public key, the Examiner respectfully disagrees. The Applicant's arguments, appearing on pages 9-10, rely upon the contention that public keys are 'generally' not kept a secret

and that Manico's security code is, and that Manico's security code is not a member of an asymmetric pair of keys. In response to the first argument, the Examiner would like to agree with the Applicant's contention, making specific note of the use of the phrase 'generally' which suggest that although *some* public key are publicly available, others are **not**. The Examiner finds it unnecessary to argue any further the issue considering the Applicant's statements already prove sufficient support.

As to the Applicant's argument concerning key pairs, the Examiner would once again like to bring to the Applicant's attention the arguments appearing on page 4 of the previous office action and relied upon for support for the use of Manico's 'security code' as a public key used to encrypt the image. The Examiner would like to remind the Applicant that claim 1 was rejected by Manico *and further in view of* Schneier as the previous office action states on page 3. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Additionally, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. the asymmetric key pair) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Applicant's next set of arguments, appearing on page 10 of the Applicant's Remarks, relate to Schneier's failure to teach 'digitizing spatially-distributed physical information' and 'digitizing a physical tag to create a digital tag'. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In the Examiner's previous office action, it was clearly stated that Manico was to be relied upon to teach 'digitizing spatially-distributed physical information', not Schneier. The Examiner would like to take this opportunity to make specific mention of the fact that the Applicant fails to argue that Manico lacks the abovementioned limitations, which is assumed to mean that the Applicant concedes that Manico does in fact disclose those limitations listed above.

Page 10 of the Applicant's remarks includes a passage summarizing the arguments above, stating that 'neither Manico nor Schneier teaches or suggest ever elemnt of claim 1 ... and this should be allowed'. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In reference to the Applicant's arguments appearing on page 11 in regards to independent claim 18, Applicant's arguments in regards to Manico's failure to teach 'a

processor adapted to read a digital tag to identify the public key' fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant's reliance upon the 'reasoning presented above in relation to claim 1' is rejected for the same reasons as presented above in relation to claim 1.

In reference to the Applicant's arguments appearing on page 12 in regards to independent claim 27, those arguments 'based on the reasoning presented above in relation to claim 1', are rejected for the reasons presented above in relation to claim 1.

Therefore, based on the above arguments, the Examiner maintains the 35 USC § 103(a) rejections as set forth below.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,373,551 B2 by Joseph Manico et al. and further in view of Bruce Schneier's "Applied Cryptography".

As per claim 1, Manico discloses a method of encrypting an image produced from physical information, comprising digitizing spatially-distributed physical information

to create a digital image of the information (col.4 lines 7-10, 22-26); digitizing a physical tag associated with the physical information (unique film id number) to create a digital tag, the digital tag being readable to identify a public key ("security code") (col.3 lines 26-29; col.4 lines 3-10); and reading the digital tag to identify the public key (col.4 lines 17-30).

Manico fails to disclose encrypting the digital image with the identified public key.

Schneier teaches a method of encrypting a digital image using a public key, to be decoded at a later time by a party in possession of the corresponding private key (pgs.31-32 reference "Communications using Public-Key Cryptography").

It would have been obvious to a person of ordinary skill in the area at the time of the invention to include within Manico's method of encrypting an image the public key method as described in Schneier to provide additional protection wherein only the party in possession of the private key, in this case the security code, is able to decode the image.

As per claim 2, Manico further discloses physically associating the physical tag with the physical information (col.3 lines 13-34).

As per claim 3, Manico further discloses including the physical information within a document, the document having a substrate that supports the physical information (col.3 lines 42-46).

As per claim 4, Manico further discloses including the physical tag on a label that is applied to the document that identifies the public key ("security code") (col.3 lines 13-34).

As per claim 5, Manico further discloses including a barcode within the physical tag (col.3 lines 44-46).

As per claim 6, Manico further discloses wherein the barcode is formed as a glyph code, and wherein the glyph code contains public-key identifying information ("security code") in a machine-readable graphic (col.3 lines 42-51; Figure 5 part 220).

As per claim 7, Manico further discloses wherein the physical tag carries the public key ("security code") (col.3 lines 13-34).

As per claim 8, Manico further discloses wherein the physical tag identifies a location on a digital storage medium, and wherein the location includes the public key ("security code") (col.4 lines 22-29).

As per claim 9, Manico further discloses sending the encrypted digital image from a sender to an address of a recipient, the address being identified by the physical tag (col.3 lines 11-25; col.4 lines 22-56).

As per claim 10, Schneier further discloses wherein sending transmitting a digital signature to the recipient, the digital signature being produced using a private key of the sender and relating to the digital image (pgs.34-41 reference "digital signature").

As per claim 11, Manico further discloses digitizing the physical tag is carried out during digitizing the physical information using a single digitizing mechanism (col.4 lines 7-10).

As per claim 12, Manico further discloses removing the digital tag from the digital image before encrypting (see Fig.7 reference "Image Storage" and "ID#/Password Database").

As per claim 13, Manico discloses a method of sending an encrypted image of a document, comprising disposing a physical tag on a document, the physical tag having a code that carries a public key ("security code") (col.3 lines 13-34); digitizing the document to create a digital image that includes a digital representation of the code (col.4 lines 7-10); and reading the digital representation of the code to obtain the public key (col.4 lines 7-10, 17-26).

Manico fails to disclose encrypting the digital image with the obtained public key and sending the encrypted image to a recipient that holds a private key, the private key forming a key pair with the public key.

Schneier teaches a method of encrypting a digital image using a public key, to be decoded at a later time by a party in possession of the corresponding private key (pgs.31-32 reference "Communications using Public-Key Cryptography").

It would have been obvious to a person of ordinary skill in the area at the time of the invention to include within Manico's method of encrypting an image the public key method as described in Schneier to provide additional protection wherein only the party in possession of the private key, in this case the security code, is able to decode the image.

As per claim 14, Manico further discloses wherein the code includes a barcode ("security code") (col.3 lines 13-34).

As per claim 15, Manico further discloses wherein the physical tag carries an address, the address corresponding to the recipient (col.3 lines 11-25; col.4 lines 22-56).

As per claim 16, Manico further discloses wherein the code is formed as a glyph code, and wherein the glyph code carries the public key ("security code") in a machine-readable graphic (col.3 lines 42-51; Figure 5 part 220).

As per claim 17, Manico further discloses wherein the physical tag is included on an adhesive label, and wherein disposing includes applying the adhesive label to the document.

As per claim 18, Manico discloses a device for encrypting an image produced from spatially-distributed physical information, the device comprising:

at least one digitizing mechanism adapted to digitize spatially-distributed physical information to create a digital image (col.4 lines 7-10, 22-26), and to digitize a physical tag associated with the physical information ("unique film id number") (col.3 lines 26-29; col.4 lines 3-10) to create a digital tag, the digital tag being readable to identify a public key ("security code") (col.4 lines 17-30); and a processor operatively connected to the digitizing mechanism and adapted to receive the digital image and digital tag from the at least one digitizing mechanism, and to read the digital tag to identify the public key (col.4 lines 17-30).

Manico fails to disclose wherein the device is capable of encrypting the image with the identified public key.

Schneier teaches a method of encrypting a digital image using a public key, to be decoded at a later time by a party in possession of the corresponding private key (pgs.31-32 reference "Communications using Public-Key Cryptography").

It would have been obvious to a person of ordinary skill in the area at the time of the invention to include within Manico's method of encrypting an image the public key method as described in Schneier to provide additional protection wherein only the party in possession of the private key, in this case the security code, is able to decode the image.

As per claim 19, Manico further discloses wherein the physical information is included in a document, the document having a substrate that supports the physical information (col.3 lines 42-46).

As per claim 20, Manico further discloses wherein the physical tag is included on a label that is applied to the document, the label having a code that identifies the public key ("security code") (col.3 lines 13-34).

As per claim 21, Manico further discloses wherein the at least one digitizing mechanism is a single mechanism that digitizes the physical tag during digitizing the physical information (col.4 lines 7-10).

As per claim 22, Manico further discloses wherein the physical tag carries an address of a recipient, and the processor is adapted to be connected to a network and to send the encrypted image to the address through the network (col.3 lines 11-25; col.4 lines 22-56).

As per claim 23, Manico further discloses wherein the physical tag includes a barcode that identifies the public key ("security code") (col.3 lines 44-46).

As per claim 24, Manico further discloses wherein the barcode is formed as a glyph code, and wherein the glyph code contains public-key identifying information ("security code") in a machine-readable graphic (col.3 lines 42-51; Figure 5 part 220).

As per claim 25, Manico further discloses wherein the physical tag carries the public key ("security code") (col.3 lines 13-34).

As per claim 26, Manico further discloses wherein the physical tag identifies a location on a digital storage medium, and wherein the location includes the public key ("security code") (col.4 lines 22-29).

As per claim 27, Manico discloses a program storage device readable by a processor, tangibly embodying a program of instructions executable by the processor to perform method steps for encrypting an image produced from physical information, comprising:

digitizing spatially-distributed physical information to create a digital image of the information (col.4 lines 7-10, 22-26);

digitizing a physical tag associated with the physical information (unique film id number) to create a digital tag, the digital tag being readable to identify a public key ("security code") (col.3 lines 26-29; col.4 lines 3-10); and reading the digital tag to identify the public key (col.4 lines 17-30).

Manico fails to disclose encrypting the digital image with the identified public key.

Schneier teaches a method of encrypting a digital image using a public key, to be decoded at a later time by a party in possession of the corresponding private key (pgs.31-32 reference "Communications using Public-Key Cryptography").

It would have been obvious to a person of ordinary skill in the area at the time of the invention to include within Manico's method of encrypting an image the public key method as described in Schneier to provide additional protection wherein only the party in possession of the private key, in this case the security code, is able to decode the image.

As per claim 28, Manico further discloses wherein the physical information is included in a document, the document having a substrate that supports the physical information (col.3 lines 42-46).

As per claim 29, Manico further discloses wherein the physical tag is included on a label that is applied to the document (col.3 lines 13-34).

As per claim 30, Manico further discloses wherein the physical tag includes a barcode that identifies the public key ("security code") (col.3 lines 44-46).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

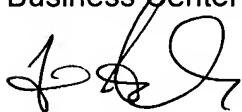
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



T.Teslovich
February 2, 2006



Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137